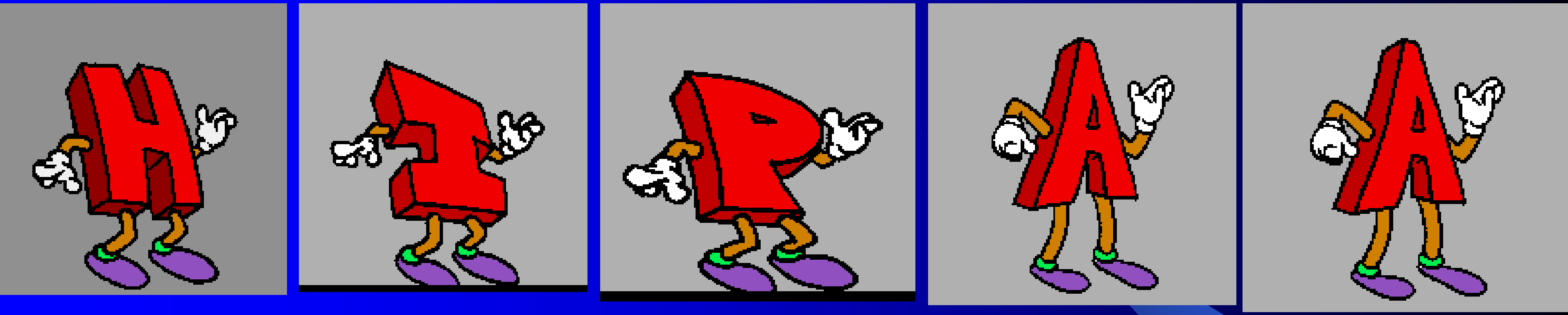


Coming soon to a Covered Entity near you!!

HIPAA Advanced Security Workshop
September 4 and 5, 2002

Edward Meyers

Interim Security Officer

Department of Mental Health

What We Hope to Accomplish

- Difference between Privacy and Security
- Administrative Procedures
- Physical Safeguards
- Technical Security Services
- Technical Security Mechanisms
- Education and Awareness
- Answer your questions

Disclaimer

The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice.

Disclaimer – Part 2

The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance.

Disclaimer – Part 3

Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to the individual listed below.

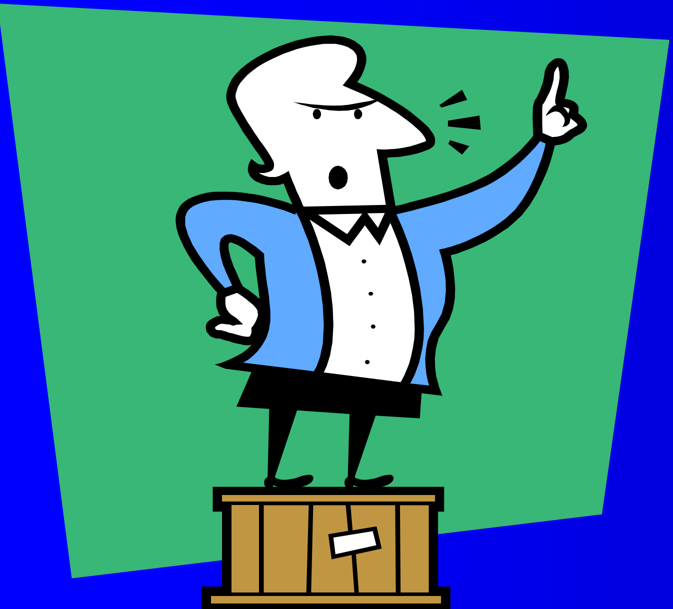
Ann Dirks-Linhorst
Privacy Officer
Missouri Department of Mental Health
314.877.0123
(Fax) 314.644.8911

Status of Final HIPAA Security Regulation

- NPRM published August 12, 1998
- Final Regulation in CMS “clearance process”
- Privacy implementation is still required by April 14, 2003

My Soapbox

- HIPAA means you too!!!
- Security is MORE than an IT issue
- Don’t forget paper records



Security, Privacy, Confidentiality

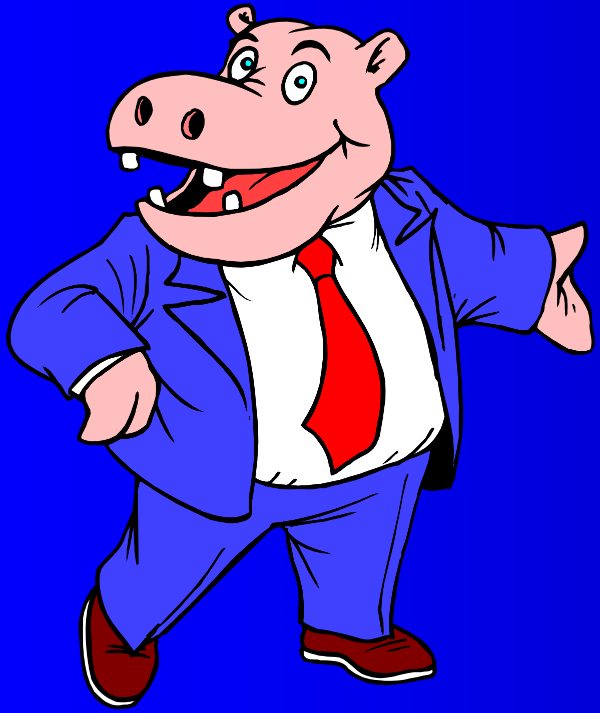
- **Security** = mechanisms to **control** access and protect systems/data from accidental or intentional access, use or disclosure to unauthorized persons

- **Privacy** = rules governing who has the **“right”** to access, use and disclose information.

- **Confidentiality** = principles governing **how** information is handled, used and disclosed.

Administrative Procedures

Purpose: To guard data integrity, confidentiality and availability



- **Contingency Plan**
  - Analysis
  - Data backup plan
  - Disaster recovery plan
  - Emergency mode operation plan
  - Testing and revision

Administrative Procedures

- **Information Access Control**
  - Access authorization
  - Access establishment
  - Access modification
- **Internal Audit**
- **Formal mechanism for processing records**

Administrative Procedures

- **Personnel Security**
  - Assure supervision of maintenance personnel by authorized, knowledgeable person
  - Maintenance of record of access authorizations
  - Operating, and in some cases, maintenance personnel have proper access authorizations
  - Personnel clearance procedure
  - Personnel security policy/procedure

Administrative Procedures

- **Termination Procedures**
  - Combination locks changed
  - Removal from access lists
  - Removal of user account(s)
  - Turn in keys, token or cards that allow access

Administrative Procedures

- **Security Configuration Management**
  - Documentation!!
  - Hardware/software installation and maintenance review and testing for security features
  - Inventory
  - Security testing
  - Virus checking

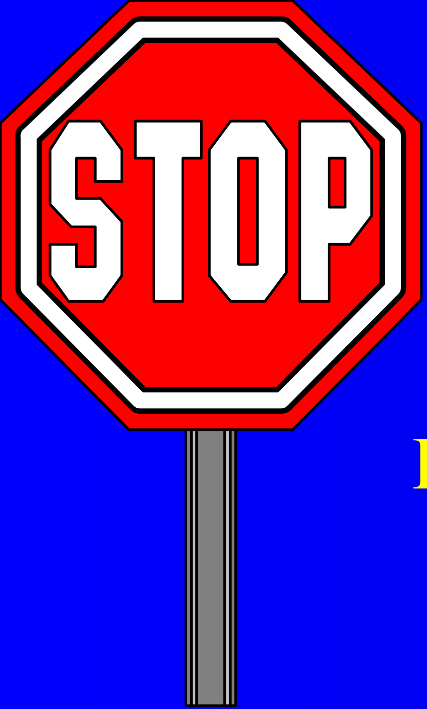
Administrative Procedures

- **Security Incident Procedures**
  - Report procedures
  - Response procedures
- **Security Management Process**
  - Risk Analysis
  - Risk management
  - Sanction policy
  - Security policy

Administrative Procedures

Other Considerations

- Assessment/Gap Analysis
- Chain of Trust Partner Agreement
- Certification
- Training



Physical Safeguards

Purpose: To guard data integrity, confidentiality and availability

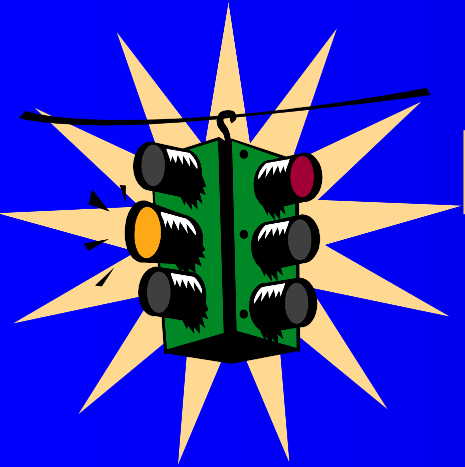
- **Media Controls**
  - Access control
  - Accountability (tracking mechanisms)
  - Data backup
  - Data storage
  - Disposal

Physical Safeguards

- **Physical Access Controls**
  - Disaster recovery
  - Emergency mode operation
  - Equipment control (into and out of site)
  - Facility security plan
  - Procedures for verifying access authorizations prior to physical access

Physical Safeguards

- **Physical Access Controls – Part 2**
  - Maintenance records
  - Need to know procedures for personnel access
  - Sign-in for visitors and escort, if appropriate
  - Testing and revision



Physical Safeguards

Other Considerations

- Assigned Security Responsibilities
- Policy/Guidelines on Work Station Use
- Secure Work Station Location
- Security Awareness Training

Technical Security Services

Purpose: To guard data integrity, confidentiality and availability

- Access Controls
  - Context-based access
  - Encryption
  - Procedure for emergency access
  - Role-based access
  - User-based access

Technical Security Services

- **Entity Authentication**
  - Automatic logoff
  - Biometric
  - Password
  - PIN
  - Telephone callback
  - Token
  - Unique user identification

Technical Security Services

Other Considerations

- Audit Controls
- Data authentication

Technical Security Mechanisms

Purpose: To guard against access to data that is transmitted over a communication network

- **Communication/network controls**
  - Access controls
  - Alarm
  - Audit trail
  - Encryption

Technical Security Mechanisms

- **Communication/network controls – part 2**
  - Entity authentication
  - Event reporting
  - Integrity controls
  - Message authentication

Education and Awareness

- **Training**
  - Awareness training for ALL personnel including management
  - Periodic security reminders
  - User education concerning virus protection
  - User education in importance of monitoring log in success/failure, and how to report discrepancies
  - User education in password management

Where to Get More Information

- DMH Web site - www.modmh.state.mo.us
- SNIP – www.mosnip.com
- Department of Health and Human Services - aspe.os.dhhs.gov/admnsimp

Questions